the described embodiment(s) for performing the same or equivalent function of the corresponding embodiment(s) without deviating therefrom. Still further, multiple processing chips or multiple devices may share the performance of one or more functions described herein, and similarly, storage may be effected across a plurality of devices. Accordingly, the disclosure is not to be limited to any single embodiment, but rather is to be construed in breadth, spirit, and scope in accordance with the appended claims.

What is claimed is:

1. A system comprising:

a datacenter configured for operation while submerged in water, the datacenter comprising one or more physically separable modules; and

an intrusion detection system coupled to the datacenter, the intrusion detection system comprising one or more intrusion detection modules that detect underwater intrusion attempts directed towards the datacenter.

2. The system of claim **1** further comprising:

a power generator, coupled to at least one of the datacenter or the intrusion detection system, that generates power from the movement of the water or air.

3. The system of claim **1** further comprising:

an energy storage module, coupled to the datacenter, that stores energy for use by the datacenter.

4. The system of claim **1** further comprising:

a compound module comprising two or more of the following: a datacenter module, a power generator module, and a power storage module.

5. The system of claim **1**, wherein the one or more intrusion detection modules further comprise one or more intrusion detection sensors.

6. The system of claim **1**, wherein the one or more intrusion detection modules include at least one of a camera, an accelerometer, a vibration sensor, a hydrophone, a sonar device, a magnetometer, a water pressure sensor, or a laser.

7. The system of claim **1**, wherein the one or more intrusion detection modules are coupled directly to the one or more physically separable modules of the datacenter.

8. The system of claim **1**, wherein the intrusion detection system includes a perimeter barrier.

9. The system of claim **8**, wherein at least a portion of the one or more intrusion detection modules is coupled to the perimeter barrier.

10. The system of claim **1**, wherein the one or more intrusion detection modules include at least one of an acoustic sensor, a pressure sensor, a vibration sensor, a temperature sensor, a voltage sensor, a current sensor, or a fiber network integrity sensor.

11. In a computing environment, a method for detecting intrusion into a datacenter submerged in water, the method performed at least in part on a processor, the method comprising:

receiving data from a plurality of sensors;

determining whether an anomaly is detected using the received data;

responsive to a determination that the anomaly is detected, identifying the anomaly;

determining whether the identified anomaly indicates an intrusion;

responsive to a determination that the detected anomaly is not an intrusion indication, outputting a change detection notice; and

responsive to a determination that the detected anomaly indicates the intrusion, initiating a search for the intrusion.

12. The method of claim **11**, wherein identifying the anomaly further comprises:

identifying a change in the environment by a distinct observation.

13. The method of claim **11**, wherein identifying the anomaly further comprises:

identifying a change in connectivity of the datacenter to a network.

14. The method of claim **11**, wherein receiving the data from the plurality of sensors further comprises:

receiving the data from one or more intrusion detection modules of an intrusion detection system associated with the datacenter.

15. The method of claim **11**, wherein receiving the data from the plurality of sensors further comprises:

receiving the data from one or more datacenter modules.

16. The method of claim **11**, wherein receiving the data from the plurality of sensors further comprises:

receiving the data from one or more remote facilities, including publicly accessible ocean or weather sensors or reports, or Automatic Identification System (AIS) reports.

17. In a computing environment, a method for performing protective actions upon detection of an intrusion into a datacenter submerged in water, the method performed at least in part on a processor, the method comprising one or more of:

triggering an alert for network operations;

broadcasting warnings into a surrounding environment;

ceasing network traffic;

failing over to a geo-replicated copy of the datacenter;

rendering data of the datacenter inaccessible.

18. The method of claim **17**, wherein broadcasting the warnings into the surrounding environment further comprises:

broadcasting the warnings into surrounding water of the datacenter using an acoustic emissions component.

19. The method of claim **17**, wherein rendering the data inaccessible further comprises rendering all in-datacenter data inaccessible, including by performing one or more of deleting all local copies of encryption keys, ignoring all network traffic pending receipt of a special sequence of packets, or powering down the datacenter.

20. The method of claim **17**, wherein rendering the data inaccessible further comprises permanently rendering all local data inaccessible, including by performing one or more of flooding the datacenter, destroying critical persistent storage structure information, or performing irreversible destructive actions on persistent data store elements.

* * * * *